CLAIMS

1. A method for securely distributing a cryptographic key, said method comprising the steps of:

combining the cryptographic key with a fresh transport key to form a key set;

unfolding a previous transport key to form an unfolded transport key;

encrypting the key set using the unfolded transport key to form an encrypted key set;

distributing the encrypted key set across a medium; and

decrypting the encrypted key set using the unfolded transport key to reconstitute the cryptographic key and the transport key.

2. The method of claim 1 wherein:

the combining, unfolding, encrypting, and distributing steps are performed by a first party; and

the decrypting step is performed by a second party in preparation for entering into secure communications with the first party.

3. The method of claim 2 wherein, prior to performing the decrypting step, the second party unfolds the previous transport key to form the unfolded transport key.

4. The method of claim 1 wherein the unfolded transport key has a volume equal to twice the volume of the previous transport key.

5. The method of claim 1 wherein the unfolding step is the reverse of a key folding process using bit swapping.

6. The method of claim 5 wherein the unfolding is performed by:

splitting each byte of the previous transport key into two new bytes;

moving most significant bits of each byte of the previous transport key into least significant bits of a new byte of the unfolded transport key; and

padding the most significant bits of each new byte of the unfolded transport key with identical bits.

7. The method of claim 1 wherein the unfolding step comprises expanding by a factor of two the size of the previous transport key by means of concatenating a common MSB sequence at uniform intervals throughout the length of said previous transport key.

8. The method of claim 1 wherein the unfolded transport key comprises bytes from a range of consecutive bytes from an ASCII character set.

9. The method of claim 8 wherein the consecutive bytes from the ASCII character set are the sixteen consecutive bytes from the ASCII character set 64 (decimal) through 79 (decimal).

10. The method of claim 1 wherein the cryptographic key is adapted for use in a One-Time Pad cipher system.

11. The method of claim 1 wherein the encrypting step and the decrypting step are performed using the same key.

12. The method of claim 1 wherein:

the steps of combining, unfolding, encrypting, distributing, and decrypting are repeated a plurality of iterations; and

the transport key from a given iteration is used to create the unfolded transport key used in the encrypting and decrypting steps in a subsequent iteration.

13. The method of claim 12 wherein the repetition of the combining, unfolding, encrypting, distributing, and decrypting steps is terminated after a preselected event has occurred.

14. The method of claim 1 wherein the encrypting step is performed using an encryption key consisting of the unfolded transport key XORed with a conversion key.

15. The method of claim 14 wherein the conversion key is a subset of the cryptographic key.

16. The method of claim 14 wherein the conversion key is generated by a true random number generator.

17. The method of claim 14 wherein the conversion key converts the unfolded transport key into a key whose bytes span a full range of an ASCII character set.

18. A computer-readable medium containing computer program instructions for securely distributing a cryptographic key, said computer program instructions performing the steps of:

combining the cryptographic key with a fresh transport key to form a key set;

unfolding a previous transport key to form an unfolded transport key;

encrypting the key set using the unfolded transport key to form an encrypted key set; and

distributing the encrypted key set across a medium.

19. Apparatus for securely distributing a cryptographic key from a first party to a second party, said apparatus comprising:

means for generating the cryptographic key;

means for generating a fresh transport key;

means for unfolding a previous transport key to form an unfolded transport key;

means for encrypting the cryptographic key and the transport key using the unfolded transport key to form an encrypted key set; and

means for enabling the first party to distribute the encrypted key set across a medium to the second party.

20. Apparatus of claim 19 further comprising means for XORing the unfolded transport key with a conversion key to create an encryption key, wherein the encryption key encrypts the cryptographic key and the transport key.